UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/765,719 | 01/26/2004 | Yolanta Beresnevichiene | 200207541-2 | 2569 |

22879          7590          01/29/2010
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

| EXAMINER |
|---|
| LOUIE, OSCAR A |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2436 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 01/29/2010 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

| | Application No. | Applicant(s) |
|---|---|---|
| **Office Action Summary** | 10/765,719 | BERESNEVICHIENE ET AL. |
| | Examiner | Art Unit | |
| | OSCAR A. LOUIE | 2436 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on <u>20 October 2009</u>.

2a) ☐ This action is **FINAL**.                2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) <u>1 and 3-41</u> is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1,3-12,17-20,22-29,31-33,36 and 38-41</u> is/are rejected.

7) ☒ Claim(s) <u>13-16,21,30,34,35 and 37</u> is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9) ☒ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a) ☐ All   b) ☐ Some * c) ☐ None of:

   1. ☐ Certified copies of the priority documents have been received.

   2. ☐ Certified copies of the priority documents have been received in Application No. _____.

   3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
  Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
  Paper No(s)/Mail. Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1.      In view of the Appeal Brief filed on 10/20/2009, PROSECUTION IS HEREBY

REOPENED.  A new grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following

two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37

CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an

appeal brief under 37 CFR 41.37.  The previously paid notice of appeal fee and appeal brief fee

can be applied to the new appeal.  If, however, the appeal fees set forth in 37 CFR 41.20 have

been increased since they were previously paid, then appellant must pay the difference between

the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing

below:

/Nasser  Moazzami/

Supervisory Patent Examiner, Art Unit 2436

2.      This non-final action is in response to the Appeal Brief filed 10/20/2009.  Claims 1 & 3-

41 are pending and have been considered as follows.

## *Specification*

3.      The specification is objected to as failing to provide proper antecedent basis for the

claimed subject matter.  See 37 CFR 1.75(d)(1) and MPEP § 608.01(o).  Correction of the

following is required:

-      Claim 39 recites "a computer program stored in a computer readable medium" but the

       claim lacks antecedent basis from the applicants' Specification.

## *Claim Rejections - 35 USC § 101*

4.      35 U.S.C. 101 reads as follows:

   Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
   any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
   requirements of this title.

5.      Claims 1, 22, & 41 rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter.

-      Claims 1 & 41 recite "a data handling apparatus" that appear to be nothing more than

       computer program modules/software, which is non-statutory subject matter under 35

       U.S.C. 101;

       **> See MPEP 2106:**
          *Descriptive material can be characterized as either "functional descriptive material"*
       *or "nonfunctional descriptive material." In this context, "functional descriptive*
       *material" consists of data structures and computer programs which impart functionality*
       *when employed as a computer component. (The definition of "data structure" is "a*
       *physical or logical relationship among data elements, designed to support specific data*
       *manipulation functions." The New IEEE Standard Dictionary of Electrical and*
       *Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but*
       *is not limited to music, literary works, and a compilation or mere arrangement of data.*

> *Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994)(discussing patentable weight of data structure limitations in the context of a statutory claim to a data structure stored on a computer readable medium that increases computer efficiency) and >In re< Warmerdam, 33 F.3d *>1354,< 1360-61, 31 USPQ2d *>1754,< 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory).*
>
> *When nonfunctional descriptive material is recorded on some computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not statutory since norequisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not makeit statutory. See >Diamond v.< Diehr, 450 U.S. *>175,< 185-86, 209 USPQ *>1,< 8(noting that the claims for an algorithm in Benson were unpatentable as abstract ideasbecause "[t]he sole practical application of the algorithm was in connection with theprogramming of a general purpose computer."). Such a result would exalt form over substance. In re Sarkar, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978) ("[E]ach invention must be evaluated as claimed; yet semantogenic considerations preclude a determination based solely on words appearing in the claims. In the final analysis under § 101, the claimed invention, as a whole, must be evaluated for what it is.") (quoted with approval in Abele, 684 F.2d at 907, 214 USPQ at 687). See also In re Johnson, 589 F.2d 1070, 1077, 200 USPQ 199, 206 (CCPA 1978) ("form of the claim is often an exercise in drafting"). Thus, nonstatutory music is not a computercomponent, and it does not become statutory by merely recording it on a compact disk Protection for this type of work is provided under the copyright law.*

Claim 22 is rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent

Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or

(2) transform underlying subject matter (such as an article or materials) to a different state or

thing.  In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184

(1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70

(1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would <u>NOT</u> qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101. *Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.*

### Claim Rejections - 35 USC § 103

6.     The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.     Claims 1, 4, 5, 22, 25-27, 39, 40, & 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>McIlroy et al.</u> ("MULTILEVEL SECURITY IN THE UNIX TRADITION").

Claim 1:

<u>McIlroy et al.</u> disclose a data handling apparatus for a computer platform using an operating system executing a process, but they do not explicitly disclose,

- "a system call monitor for detecting predetermined system calls and data manipulated by the process so as to modify identifiable characteristics of the data," although McIlroy et al. do suggest an operating system security framework that monitors process system calls that access files, as recited below;

- "means for applying a data handling policy upon detecting: a predetermined data type based on a tag or label associated with the data manipulated by the process or based on the format of the data manipulated by the process," although McIlroy et al. do suggest file labels associated with a per process access policy, as recited below;

- "a predetermined system call which involves the writing of data outside the process," although McIlroy et al. do suggest process system call file access externally across a network as well as internally via a pipe or file stream, as recited below;

however, McIlroy et al. do disclose,

- [pages 4-5 describe a framework which monitors system calls made by at least one process to access a file for reading/writing/etc.];

- [pages 2-5 describe a framework which monitors system calls made by at least one process to access a file for reading/writing/etc., where the files have labels that are checked to determine the security policy which is applied to the process attempting to execute an operation on the file];

- [pages 8-9 describe process system call paths for accessing files as including those of internal file streams/pipes as well as external paths such as network communications between two or more computers];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "a system call monitor for detecting predetermined system calls

and data manipulated by the process so as to modify identifiable characteristics of the data" and

"means for applying a data handling policy upon detecting: a predetermined data type based on a

tag or label associated with the data manipulated by the process or based on the format of the

data manipulated by the process" and "a predetermined system call which involves the writing of

data outside the process," in the invention as disclosed by McIlroy et al. for the purposes of

providing process file access control based on labels associated with a policy.

Claim 4:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 1 above, further comprising,

- "predetermined system calls are those involving the transmission of data externally of the

    computing platform" [pages 8-9 describe process system call paths for accessing files as

    including those of internal file streams/pipes as well as external paths such as network

    communications between two or more computers].

Claim 5:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 1 above, further comprising,

- "means for applying a data handling policy comprises a tag determiner for determining

    any security tags associated with the data manipulated by the process or based on the

    format of the data manipulated by the process handled by the system call" and "means for

    applying a data handling policy comprises a policy interpreter for determining a policy

according to any such tags and for applying the policy" [pages 2-5 describe a framework

which monitors system calls made by at least one process to access a file for

reading/writing/etc., where the files have labels that are checked to determine the security

policy which is applied to the process attempting to execute an operation on the file].

Claim 22:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, but they do not explicitly disclose,

-   "detecting both a predetermined data type based on a tag or label associated with the data

    or based on the format of the data," although McIlroy et al. do suggest an operating

    system security framework that monitors process system calls that access files by

    utilizing labels associated with a policy, as recited below;

-   "predetermined system calls involving the writing of data outside the process," although

    McIlroy et al. do suggest process system call file access externally across a network as

    well as internally via a pipe or file stream, as recited below;

-   "applying a data handling policy to a system call upon both said predetermined data type

    and said predetermined system call being detected," although McIlroy et al. do suggest

    file labels associated with a per process access policy, as recited below;

-   "the data handling policy being applied for all system calls involving the writing of data

    outside the process," although McIlroy et al. do suggest process system call file access

    externally across a network as well as internally via a pipe or file stream, as recited

    below;

however, McIlroy et al. do disclose,

-   [pages 4-5 describe a framework which monitors system calls made by at least one

    process to access a file for reading/writing/etc.];

-   [pages 2-5 describe a framework which monitors system calls made by at least one

    process to access a file for reading/writing/etc., where the files have labels that are

    checked to determine the security policy which is applied to the process attempting to

    execute an operation on the file];

-    [pages 8-9 describe process system call paths for accessing files as including those of

    internal file streams/pipes as well as external paths such as network communications

    between two or more computers];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "detecting both a predetermined data type based on a tag or

label associated with the data or based on the format of the data" and "predetermined system

calls involving the writing of data outside the process" and "applying a data handling policy to a

system call upon both said predetermined data type and said predetermined system call being

detected" and "the data handling policy being applied for all system calls involving the writing

of data outside the process," in the invention as disclosed by McIlroy et al. for the purposes of

providing process file access control based on labels associated with a policy.

Claim 25:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 22 above, further comprising,

- "predetermined system calls are those involving the transmission of data externally of the

  computing platform" [pages 8-9 describe process system call paths for accessing files as

  including those of internal file streams/pipes as well as external paths such as network

  communications between two or more computers].

Claim 26:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 22 above, further comprising,

- "determining any security tags associated with data handled by the system call" and

  "determining a policy according to any such tags and applying the policy" [pages 2-5

  describe a framework which monitors system calls made by at least one process to access

  a file for reading/writing/etc., where the files have labels that are checked to determine

  the security policy which is applied to the process attempting to execute an operation on

  the file].

Claim 27:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 22 above, further comprising,

- "a composite policy is generated from the tag policies relevant to the data" [pages 2-5

    describe a framework which monitors system calls made by at least one process to access

    a file for reading/writing/etc., where the files have labels that are checked to determine

    the security policy which is applied to the process attempting to execute an operation on

    the file].

Claims 39 & 40:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 22 above, further comprising,

- "a computer program stored in computer readable media for controlling a computing

    platform to operate in accordance with claim 22" and "a computer platform configured to

    operate according to claim 22" [page 2 describes several computers].

Claim 41:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, but they do not explicitly disclose,

- "a system call monitor for detecting predetermined system calls and data handled by the process," although <u>McIlroy et al.</u> do suggest an operating system security framework that monitors process system calls that access files by utilizing labels associated with a policy, as recited below;

- "a policy applicator for applying a data handling policy to the system call upon both a predetermined data type based on a tag or label associated with the data handled by the process or based on the format of the data handled by the process," although <u>McIlroy et al.</u> do suggest file labels associated with a per process access policy, as recited below;

- "a predetermined system call which involves the writing of data outside the process," although <u>McIlroy et al.</u> do suggest process system call file access externally across a network as well as internally via a pipe or file stream, as recited below;

however, <u>McIlroy et al.</u> do disclose,

- [pages 4-5 describe a framework which monitors system calls made by at least one process to access a file for reading/writing/etc.];

- [pages 2-5 describe a framework which monitors system calls made by at least one process to access a file for reading/writing/etc., where the files have labels that are checked to determine the security policy which is applied to the process attempting to execute an operation on the file];

- [pages 8-9 describe process system call paths for accessing files as including those of internal file streams/pipes as well as external paths such as network communications between two or more computers];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "a system call monitor for detecting predetermined system calls

and data handled by the process" and "a policy applicator for applying a data handling policy to

the system call upon both a predetermined data type based on a tag or label associated with the

data handled by the process or based on the format of the data handled by the process" and

"applying a data handling policy to a system call upon both said predetermined data type and

said predetermined system call being detected" and "a predetermined system call which involves

the writing of data outside the process," in the invention as disclosed by McIlroy et al. for the

purposes of providing process file access control based on labels associated with a policy.

8.      Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over McIlroy et al.

("MULTILEVEL SECURITY IN THE UNIX TRADITION") in view of Paul C. Clark ("Policy-

Enhanced Linux").

Claim 7:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 1 above, further comprising,

-       "the policy interpreter comprises a policy database including tag policies" and "the policy

        interpreter comprises a policy reconciler for generating a composite policy from the tag

        policies relevant to the data" [sections 2.1.2, 2.2.3, & 2.2.4 describe policy label

        databases and an associated manager].

9.      Claims 3, 6, 23, 24, & 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over

McIlroy et al. ("MULTILEVEL SECURITY IN THE UNIX TRADITION") in view of Choo

(US-6981140-B1).

Claim 6:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 5 above, but they do not explicitly disclose,

-    "the policy interpreter is configured to use the intended destination of the data as a factor

     in determining the policy for the data," although Choo does suggest policy

     enforcement/access control based on where data packets come from, as recited below;

however, Choo does disclose,

-    "For incoming data packets received from the remote host across a LAN/WAN each

     packet received from the operating system is inspected to see if internet protocol security

     decryption is necessary by examining a security descriptor data comprising a part of a

     security association data logically associated with the data packet" [column 12 lines 54-

     59];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the policy interpreter is configured to use the intended

destination of the data as a factor in determining the policy for the data," in the invention as

disclosed by McIlroy et al. for the purposes of enforcing policies/access control.

Claim 23:

McIlroy et al. disclose a data handling apparatus and method for a computer platform using an

operating system executing a process, as in Claim 22 above respectively, but they do not

explicitly disclose,

-    "the policy is to require the encryption of at least some of the data," although Choo does

     suggest encryption of data, as recited below;

however, <u>Choo</u> does disclose,

- "the security database associated with key database 602 is consulted to determine

  whether the data packet received from user process 600 is to be encrypted prior to

  transmission across the network" [column 13 lines 14-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the policy is to require the encryption of at least some of the

data," in the invention as disclosed by <u>McIlroy et al.</u> for the purposes of securing the data.

Claims 3 & 24:

<u>McIlroy et al.</u> disclose a data handling apparatus and method for a computer platform using an

operating system executing a process, as in Claims 1 and 23 above respectively, but they do not

explicitly disclose,

- "the policy interpreter in its application of the policy automatically encrypts the at least

  some of the data," although <u>Choo</u> does suggest encryption of data, as recited below;

however, <u>Choo</u> does disclose,

- "the security database associated with key database 602 is consulted to determine

  whether the data packet received from user process 600 is to be encrypted prior to

  transmission across the network" [column 13 lines 14-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "a policy interpreter in its application of the policy

automatically encrypts the at least some of the data," in the invention as disclosed by McIlroy et

al. for the purposes of securing the data.


Claim 28:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 26 above, but they do not explicitly disclose,

- "the intended destination of the data is used as a factor in determining the policy for the

  data," although Choo does suggest policy enforcement/access control based on where

  data packets come from, as recited below;

however, Choo does disclose,

- "For incoming data packets received from the remote host across a LAN/WAN each

  packet received from the operating system is inspected to see if internet protocol security

  decryption is necessary by examining a security descriptor data comprising a part of a

  security association data logically associated with the data packet" [column 12 lines 54-

  59];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the intended destination of the data is used as a factor in

determining the policy for the data," in the invention as disclosed by McIlroy et al. for the

purposes of enforcing policies/access control.

10.    Claims 8-12, 17-20, 29, 31-33, & 36 are rejected under 35 U.S.C. 103(a) as being

unpatentable over McIlroy et al. ("MULTILEVEL SECURITY IN THE UNIX TRADITION")

in view of Yoshioka et al. (US-5909688-A).

Claims 8 & 29:

McIlroy et al. disclose a data handling apparatus and method for a computer platform using an

operating system executing a process, as in Claims 1 and 22 above respectively, but they do not

explicitly disclose,

-    "the computing platform comprises a data management unit," although Yoshioka et al. do

     suggest a data management unit, as recited below;

-    "the data management unit arranged to associate data management information with data

     input to a process," although Yoshioka et al. do suggest entity information corresponding

     with each record, as recited below;

-    "(the data management unit arranged to) regulate operating system operations involving

     the data according to the data management information," although Yoshioka et al. do

     suggest controlling read/write of data, as recited below;

however,  Yoshioka et al. do disclose,

-    [Fig 13 illustrates a data management unit];

-    "in a record of department in an entity management table corresponding to the above-

     mentioned organization template there are stored entity information corresponding to that

     record, an XID value of, for example, a technical department, a pointer to a section

record which is a low-rank record, a pointer to a record for another department which is

in the same rank as that department, and a pointer to that department which is the entity

information item" [column 6 lines 9-17];

- " The data management unit 24 controls reading or writing of data between the database

25 and the memory 31" [column 12 lines 65-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the computing platform comprises a data management unit"

and "the data management unit arranged to associate data management information with data

input to a process" and "(the data management unit arranged to) regulate operating system

operations involving the data according to the data management information," in the invention as

disclosed by McIlroy et al. for the purposes of associating and tracking data processed in an

operating system.

Claim 9:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 8 above, but they do not explicitly disclose,

- "the computing platform further comprises a memory space," although Yoshioka et al. do

suggest a memory, as recited below;

- "the computing platform is arranged to load the process into the memory space,"

although Yoshioka et al. do suggest a memory connected to other components for data

processes, as recited below;

- "the computing platform is arranged to run the process under the control of the data

  management unit," although <u>Yoshioka et al.</u> do suggest a data management unit, as

  recited below;

however, <u>Yoshioka et al.</u> do disclose,

- [Fig 13 illustrates a memory arranged with other components to load and handle data

  processes and a data management unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the computing platform further comprises a memory space"

and "the computing platform is arranged to load the process into the memory space" and "the

computing platform is arranged to run the process under the control of the data management

unit," in the invention as disclosed by <u>McIlroy et al.</u> for the purposes of loading a process into

memory and handling the execution of that process according to a policy, as are common

elements of an operating system's functionality when incorporated according to a system as

shown in Fig 13 of <u>Yoshioka et al</u>.

Claim 10:

<u>McIlroy et al.</u> disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 8 above, but they do not explicitly disclose,

- "the data management information is associated with at least one data sub-unit as data is

  input to a process from a data unit comprising a plurality of sub-units," although

  <u>Yoshioka et al.</u> do suggest a data management unit connected to additional components,

  as recited below;

however,  Yoshioka et al. do disclose,

- [Fig 13 illustrates a system with a data management unit and several sub-units defining

  aspects of policy, work-flow, etc interfaced with an interface unit, a database, and a

  memory];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the data management information is associated with at least

one data sub-unit as data is input to a process from a data unit comprising a plurality of sub-

units," in the invention as disclosed by McIlroy et al. since the data management unit would

associate data according to the policies of the subunits as data input for the purposes of handling

data processing.

Claim 11:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 8 above, but they do not explicitly disclose,

- "data management information is associated with each independently addressable data

  unit," although Yoshioka et al. do suggest a data management unit controlling the

  read/write of data involving memory, as recited below;

however,  Yoshioka et al. do disclose,

- "The data management unit 24 controls reading or writing of data between the database

  25 and the memory 31" [column 12 lines 65-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "data management information is associated with each

independently addressable data unit," in the invention as disclosed by McIlroy et al. since the

data management unit would have some association or elements of data identification for the

purposes of reading/writing data between a database and memory.

Claim 12:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 8 above, but they do not explicitly disclose,

- "the data management unit comprises part of an operating system kernel space," although

    Yoshioka et al. do suggest a data management unit, as recited below;

however, Yoshioka et al. do disclose,

- "The data management unit 24 controls reading or writing of data between the database

    25 and the memory 31" [column 12 lines 65-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the data management unit comprises part of an operating

system kernel space," in the invention as disclosed by McIlroy et al. since reading/writing to

memory and between a database is typically an operation reserved for kernel space privileges,

for the purposes of resource access control within the operating system.

Claim 17:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 8 above, but they do not explicitly disclose,

- "the data management unit comprises a data filter to identify data management

   information associated with data that is to be read into the memory space," although

   Yoshioka et al. do suggest a data management unit reading/writing data between a

   database and memory, as recited below;

however, Yoshioka et al. do disclose,

- "The data management unit 24 controls reading or writing of data between the database

   25 and the memory 31" [column 12 lines 65-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the data management unit comprises a data filter to identify

data management information associated with data that is to be read into the memory space," in

the invention as disclosed by McIlroy et al. since the data management unit would have to have

some association or elements of data identification in order to read/write data between the

database and memory, for the purposes of ensuring data integrity/consistency between what is in

memory and what is written in the database.

Claim 18:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 8 above, but they do not explicitly disclose,

- "the data management unit further comprises a tag management module arranged to

  allow a user to specify data management information to be associated with data,"

  although Yoshioka et al. do suggest a data management unit connected to an interface

  unit, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates an interface unit interfaced with the data management unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the data management unit further comprises a tag management

module arranged to allow a user to specify data management information to be associated with

data," in the invention as disclosed by McIlroy et al. for the purpose of allowing additional

policies/control over the data management unit.

Claim 19:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating

system executing a process, as in Claim 8 above, but they do not explicitly disclose,

- "the data management unit comprises a tag propagation module arranged to maintain an

  association with the data that has been read into the process and the data management

  information associated therewith," although Yoshioka et al. do suggest a data

  management unit connected with several additional components for data management, as

  recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit interfaced with a database, memory, and several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the data management unit comprises a tag propagation module arranged to maintain an association with the data that has been read into the process and the data management information associated therewith," in the invention as disclosed by McIlroy et al. since the data management unit would have to have some association or elements of data identification in order to read/write data between the database and memory for the purposes of data integrity/consistency between data in memory and the data written in the database.

Claim 20:

McIlroy et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 19 above, but they do not explicitly disclose,

- "the tag propagation module is arranged to maintain an association between an output of operations carried out within the process and the data management information associated with the data involved in the operations," although Yoshioka et al. do suggest a data management unit in association with a policy unit, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit interfaced with a database, memory, and several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the tag propagation module is arranged to maintain an

association between an output of operations carried out within the process and the data

management information associated with the data involved in the operations," in the invention as

disclosed by McIlroy et al. since the data management unit would have to have some association

or elements of data identification in order to read/write data between the database and memory

for the purposes of data integrity/consistency between data in memory and the data written in the

database, as well as, access control for the data.

Claim 31:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 29 above, but they do not explicitly disclose,

-    "associating data management information with data as the data is read into a memory

     space," although Yoshioka et al. do suggest a data management unit in association with a

     policy unit and a memory, as recited below;

however, Yoshioka et al. do disclose,

-    [Fig 13 illustrates a data management unit interfaced with a database, memory, and

     several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "associating data management information with data as the data

is read into a memory spaces," in the invention as disclosed by McIlroy et al. since the data

management unit would have to have some association or elements of data identification in order to read/write data between the database and memory for the purposes of data integrity/consistency in memory.

Claim 32:

McIlroy et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 29 above, but they do not explicitly disclose,

- "associating data management information with at least one data sub-unit as data is read into a memory space from a data unit comprising a plurality of data sub-units," although Yoshioka et al. do suggest a data management unit in association with a policy unit and a memory, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit interfaced with a database, memory, and several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "associating data management information with at least one data sub-unit as data is read into a memory space from a data unit comprising a plurality of data sub-units," in the invention as disclosed by McIlroy et al. since the data management unit would have to have some association or elements of data identification in order to read/write data between the database and memory for the purposes of data integrity/consistency between data in memory and the data written in the database, as well as, access control for the data.

Claim 33:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 29 above, but they do not explicitly disclose,

-   "associating data management information with each independently addressable data unit

    that is read into the memory space," although Yoshioka et al. do suggest a data

    management unit in association with a memory, as recited below;

however,  Yoshioka et al. do disclose,

-   [Fig 13 illustrates a data management unit interfaced with a database, memory, and

    several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "associating data management information with each

independently addressable data unit that is read into the memory space," in the invention as

disclosed by McIlroy et al. since the data management unit would have to have some association

or elements of data identification in order to read/write data between the database and memory.

Claim 36:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 29 above, but they do not explicitly disclose,

-   "the step (b) comprises sub-steps," although Yoshioka et al. do suggest a database in

    association with additional sub-components including a policy unit, as recited below;

-   "identifying an operation involving the data," although Yoshioka et al. do suggest a

    database in association with additional sub-components including a policy unit, as recited

    below;

- "if the operation involves the data and is carried out within the process, maintaining an

  association between an output of the operation and the data management information,"

  although Yoshioka et al. do suggest a database in association with additional sub-

  components including a policy unit, as recited below;

- "if the operation involving the data includes a write operation to a location external to the

  process, selectively performing the operation dependent on the data management

  information," although Yoshioka et al. do suggest a database in association with

  additional sub-components including a policy unit, as recited below;

however, Yoshioka et al. does disclose,

- [Fig 14 illustrates several subunits that perform sub-steps and interact with a database];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the step (b) comprises sub-steps" and "identifying an operation

involving the data" and "if the operation involves the data and is carried out within the process,

maintaining an association between an output of the operation and the data management

information" and "if the operation involving the data includes a write operation to a location

external to the process, selectively performing the operation dependent on the data management

information," in the invention as disclosed by McIlroy et al. since database read/write sessions

typically involve multiple steps (i.e. sub-steps) and involve data operations. In addition, the data

management unit would have some association or elements of data identification in order to

read/write data between the database and memory for the purposes of maintaining data

integrity/consistency between data in memory and data written in the database, as well as, for the

access control of data processing operations by the policy unit.

11.     Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over McIlroy et al.

("MULTILEVEL SECURITY IN THE UNIX TRADITION") in view of Johnson et al. (US-

5684948-A).

Claim 38:

McIlroy et al. disclose a data handling method for a computer platform using an operating

system executing a process, as in Claim 29 above, but they do not explicitly disclose,

-   "the process instructions are analyzed as blocks," although Johnson et al. do suggest

    addressable privilege levels of code in each address block, as recited below;

-   "each block defined by operations up to a terminating condition," although Johnson et al.

    do suggest bit sets indicating privilege levels, as recited below;

however,  Yoshioka et al. does disclose,

-   "the privilege level of the code (and/or data) in each of a plurality of address blocks

    addressable by the processor" [column 2 lines 41-42];

-   "The bit being set indicates that the corresponding address block has one privilege level

    and the bit being cleared indicates that the corresponding address block has the other

    privilege level" [column 2 lines 46-48];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the process instructions are analyzed as blocks" and "each

block defined by operations up to a terminating condition," in the invention as disclosed by

McIlroy et al. since process instructions are typically handled as blocks by a processor and would

have a condition for completion.

### *Allowable Subject Matter*

12.    Claims 13-16, 21, 30, 34, 35 & 37 are objected to as being dependent upon a rejected

base claim, but would be allowable if rewritten in independent form including all of the

limitations of the base claim and any intervening claims.

### *Conclusion*

13.    The prior art made of record and not relied upon is considered pertinent to the applicant's

disclosure.

      a.      <u>Chris M. Wright</u> ("Proceedings of the Ottawa Linux Symposium") – pages 64-

      617;

      b.      <u>Cohen et al.</u> (US 20050076237 A1/US 7437766 B2) - method and apparatus

      providing deception and/or altered operation in an information system operating system;

      c.      <u>Choo</u> (US 20030145235 A1) - network adapter management;

14.    Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684.

The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

      If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami, can be reached at 571-272-4195.  The fax phone number for

Formal or Official faxes to Technology Center 2400 is 571-273-8300.

      Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system.  Status information for published applications

may be obtained from either Private PAIR or Public PAIR.  Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you

would like assistance from a USPTO Customer Service Representative or access to the

automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


                    /OSCAR A LOUIE/
                       01/22/2010


/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436